

RESEARCH ARTICLE

On The Secrecy of the Cognitive Interference Channel with Partial Channel States

Hamid G. Bafghi[†], Babak Seyfe[†], Mahtab Mirmohseni[‡], Mohammad Reza Aref[‡]

[†] Information Theoretic Learning System Lab. (ITLSL), Department of Electrical Engineering, Shahed University, Tehran, Iran.

[‡] Information Systems and Security Lab. (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran.
E-mails: {ghanizade, seyfe}@shahed.ac.ir, {mirmohseni, aref}@sharif.edu.

ABSTRACT

The secrecy problem in the state-dependent cognitive interference channel is considered in this paper. In our model, there are a primary and a secondary (cognitive) transmitter-receiver pairs, in which the cognitive transmitter has the message of the primary one as side information. In addition, the channel is affected by a channel state sequence which is estimated partially at the cognitive transmitter and the corresponding receiver, separately. The cognitive transmitter should cooperate with the primary one, and it wishes to keep its message secure at the primary receiver. The achievable equivocation-rate regions for this channel are derived using two approaches: the binning scheme coding, and superposition coding. Then the outer bounds on the capacity are derived and the results are extended to the Gaussian examples. Copyright © 2016 John Wiley & Sons, Ltd.

1. INTRODUCTION

Interference channel, in which the intended signal for one receiver causes interference at the other receivers, is a basic model to study the constraints on the practical communication networks [1]. The Cognitive Interference Channel (CIC) is one case of the interference channels in which one of the transmitter-receiver pair, namely the primary one, has the privileges to use the channel [2, 3]. The secondary transmitter-receiver pair, i. e., the cognitive one, uses the channel without causing problem for the primary one. In one approach, the cognitive transmitter cooperates with the primary party by spending the cognition cost [4]. Although the capacity of this channel remains an open problem in general case, many works studied the achievable rate region for this channel [5–8]. Under degradedness condition, [5] derived the capacity for the CIC. The achievable rate of [4] is improved by [6–9].

The nature of the interference channel causes to leak the information to unintended destinations. In the information theory literature, secure communication between the transmission parties was first studied in [10] by Shannon. Afterwards, Wyner introduced the wiretap channel to model the secrecy problem in the physical layer [11]. Furthermore, he proposed the *Random Coding* to keep the sent message away from the eavesdropper. This coding scheme is based on the fact that a receiver cannot decode any information more than its channel capacity with low-enough error probability. Recently, there has

been a significant interest in the secrecy of multi-users systems [12] with a particular emphasis on the secrecy of the CIC [2, 13, 14]. The works [2, 13, 14] derived some equivocation-rate regions for the CIC to show the trade off between the achievable rate and the secrecy level in this channel.

Modeling a time-varying channel, whose instantaneous parameters depend on a random state sequence, is introduced and studied by Shannon in his landmark paper [15]. Moreover, the knowledge of the random state sequence, i. e., the Channel State Information (CSI) is assumed to be available at the transmitter in [15]. There are considerable research interests in studying the effect of the CSI in various channel models (see [16] and the references therein). Specifically, the capacity of a discrete memoryless point to point channel with non-causal CSI available at the Transmitter (CSIT) is derived by Gel'fand and Pinsker [17], and it is extended to the Gaussian channel in [18]. The CIC with CSI available at the cognitive transmitter is studied in [3, 19] and the equivocation-rate region on this model is derived by [20]. Moreover, some works consider the impact of partial channel state information on the capacity and performance of the cognitive radio [21, 22].

In this paper, we study the CIC with Partial Channel State information (CIC-PCSI). The partial CSIs are assumed to be known non-causally at the cognitive transmitter and the corresponding receiver (see Figure 1). Here, the cognitive transmitter should mitigate its

interference at the primary receiver. Furthermore, it wishes to keep its message confidential with respect to the primary receiver.

The CIC-PCSI model can be motivated by the wireless sensor network application with different sensor types [5], in which one sensor has a better sensing capability than the other one. The simpler sensor provides one event to its corresponding destination, but the more capable sensor which can sense two events, cooperates with the simpler sensor. Since the more capable sensor senses a vital event, it wishes to keep its message confidential at the destination of the simpler sensor. Moreover, the channel is affected by a channel state sequence which is estimated at the more capable sensor and its destination, separately [23]. These estimated observations of the channel state sequence are not equal to each other in general case.

We study the different effects of the CSIT and CSIR on two coding schemes to achieve the equivocation-rate region. For this aim, we use the *Binning scheme* [6, 24, 25] and the *Superposition Coding* [2, 3, 20] in CIC-PCSI. In the binning scheme, the cognitive transmitter, after rate splitting, bins its message against the code-book of the primary one. Then, it superimposes its message on the primary transmitter's message and the channel state sequence. In the superposition scheme, the cognitive transmitter superimposes its message on the primary transmitter's message and the channel state sequence. In each scheme, random coding is used to guaranty the secrecy condition for the cognitive transmitter's message [11]. Then, the outer bounds on the capacity of the CIC-PCSI are proposed. Moreover, we extend the results of two cases, i.e., binning scheme and superposition coding, to the Gaussian model, and it is shown that the cognitive transmitter can choose the best coding scheme to maximize the achievable equivocation-rate region. In comparison of our model with the different ones in [3, 6, 24, 25], we consider secrecy constraints in the CIC. Since we assume that the primary transmitter's message is fully known at the cognitive transmitter, the secrecy issue is considered for the cognitive transmitter's message (see the similar model in [2]). Furthermore, in compare with the model of [13] and [14], the CSI knowledge enhances the cognitive transmitter to improve the equivocation-rate region.

The rest of the paper is as follows. In Section 2, the channel model and some preliminaries and the definitions are explained. In Section 3, the main results on the achievable equivocation-rate region using the binning scheme are proposed. Furthermore, in this section we derive the proper outer bounds on the capacity, and extend the results to the Gaussian case. In Section 4, using the superposition coding, we derive the equivocation-rate region and an outer bound on the capacity of the channel. Then, we extend the results to the Gaussian channel as an example. Finally, the paper is concluded in Section 5. The proofs of the theorems are relegated to the appendices.

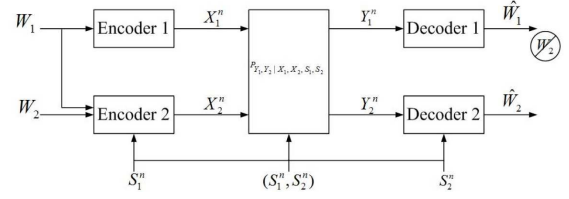


Figure 1: The cognitive interference channel with two partial channel states information available at the transmitter and the receiver, with a confidential message.

2. CHANNEL MODEL AND PRELIMINARIES

2.1. The Notation

First, we explain the notation. We use \mathcal{X} to denote a finite alphabet with cardinality $|\mathcal{X}|$. $x^n = \{x_1, x_2, \dots, x_n\}$ represents the members of \mathcal{X}^n , in which the subscripted and superlative letters represent the components and the vectors, respectively. x_i^j is used to indicate the vector (x_i, \dots, x_j) . For the random vectors and the random variables, which are denoted by uppercase letters, a similar convention is used.

2.2. Channel Model

Consider a memoryless stationary state-dependent interference channel with finite input alphabets \mathcal{X}_1 and \mathcal{X}_2 , finite output alphabets \mathcal{Y}_1 and \mathcal{Y}_2 , the channel states alphabets $\mathcal{S}_1, \mathcal{S}_2$ with distribution $\mathcal{P}_{S_1}, \mathcal{P}_{S_2}$ and a conditional probability distribution $P_{Y_1, Y_2 | X_1, X_2, S_1, S_2}$. As shown in the Figure 1, the t -th transmitter, where $t = 1, 2$, wishes to transmit the message W_t which is uniformly distributed on the set $\mathcal{W}_t \in \{1, \dots, M_t\}$. The message W_1 is assumed to be known at both transmitters, but the message W_2 is just known at the transmitter 2 (the cognitive transmitter). Furthermore, it is assumed that the channel is dependent on two channel states. One of these channel states, i.e., S_1 , is assumed to be known non-causally at the cognitive transmitter. The other one, i.e., S_2 , is assumed to be known non-causally at the cognitive destination. Thus, the cognitive party wishes to increase its achievable rate using this side information.

Given the inputs and the states, i.e., the n -sequences $X_1^n, X_2^n, S_1^n, S_2^n$, the conditional distribution of the channel outputs n -sequences Y_1^n, Y_2^n take the product form as follows

$$P_{Y_1^n, Y_2^n | X_1^n, X_2^n, S_1^n, S_2^n}(y_1^n, y_2^n | x_1^n, x_2^n, s_1^n, s_2^n) = \prod_{i=1}^n P_{Y_1, Y_2 | X_1, X_2, S_1, S_2}(y_{1,i}, y_{2,i} | x_{1,i}, x_{2,i}, s_{1,i}, s_{2,i}) \quad (1)$$

2.3. Definitions

An (M_1, M_2, n, P_e) -code has two encoding-decoding functions and an error probability. The encoding functions

are defined as

$$\begin{aligned}\varphi_{1,n} &: \mathcal{W}_1 \rightarrow \mathcal{X}_1^n, \\ \varphi_{2,n} &: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}_1^n \rightarrow \mathcal{X}_2^n,\end{aligned}\quad (2)$$

and the channel decoders are defined by the mappings

$$\begin{aligned}\psi_{1,n} &: \mathcal{Y}_1^n \rightarrow \hat{\mathcal{W}}_1, \\ \psi_{2,n} &: \mathcal{Y}_2^n \times \mathcal{S}_2^n \rightarrow \hat{\mathcal{W}}_2.\end{aligned}\quad (3)$$

The error probability $P_e = \max(P_{e,1}, P_{e,2})$ is defined as

$$P_{e,t} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} P[\hat{w}_t \neq w_t | w_1, w_2 \text{ were sent}]. \quad (4)$$

Definition 1

The secrecy level of the cognitive transmitter's message at the primary receiver (receiver 1) is measured by normalized equivocation-rate which is defined as

$$R_{e_2}^{(n)} = \frac{1}{n} H(W_2 | Y_1^n), \quad (5)$$

which is known as the "weak secrecy condition" [12].

Definition 2

The equivocation-rate-triple (R_1, R_2, R_{e_2}) is an achievable region if for any $\epsilon_n > 0$ there exists an (M_1, M_2, n, P_e) code such that $M_i \geq 2^{nR_i}$, $i = 1, 2$ for which we have $P_e \leq \epsilon_n$, and

$$0 \leq R_{e_2} \leq \liminf_{n \rightarrow \infty} R_{e_2}^{(n)}. \quad (6)$$

Definition 3

The capacity region is the closure of the set of all achievable equivocation-rate regions.

2.4. Encoding Schemes

Now, we discuss the rate achieving encoding schemes we will use in the CIC problem. First, consider a point-to-point state-dependent communication system in which the CSI is known non-causally at the transmitter. Assume that the channel state sequence S plays the role of the interference signal which can be considered as a code-book with rate $R_S = I(Y; S)$. The transmitter wishes to transmit the message W at the rate R through the channel. There are two coding schemes to achieve the rate region: *Superposition Coding* (SPC) and *Gel'fand-Pinsker Coding* (GPC); depending on the interference's rate R_S , either one may be chosen. When R_S is small, we can improve the achievable rate using the SPC. For higher R_S , we can achieve the rate using the classical GPC. The following lemma expresses the result using these two coding schemes [6, Lemma 1]. This lemma is used to derive the achievable rate regions for the CIC-PCSI in the next sections.

Lemma 1

[6, Lemma 1] The following rate region is achievable for a point to point communication system with non-causal CSIT

$$\begin{aligned}R &\leq \max_{P_{U|S}, f(\cdot)} \min\{I(X; Y|S), \\ &\max\{I(U; S; Y) - R_S, I(U; Y) - I(U; S)\}\}. \quad (7)\end{aligned}$$

Outline of the proof

For the case $I(S; U, Y) \leq R_S \leq H(S)$, the binning scheme achieves the rate given by the second term of (7). For $R_S \leq I(S; U, Y)$, SPC achieves the rate region by the first term in (7). For more details we refer to [6, Lemma 1]. \square

3. USING THE BINNING SCHEME

In this section we derive the achievable equivocation-rate region for the CIC-PCSI, shown in Figure 1, using the binning scheme. Then, two outer bounds on the capacity are proposed, and the results are extended to the Gaussian channel as special case.

3.1. An inner bound

To derive an achievable rate region for this channel, we use the rate splitting as follows.

$$R_1 = R_{1a} + R_{1b}, \quad (8)$$

$$R_2 = R_{2a} + R_{2b}, \quad (9)$$

for non-negative rates R_{1a}, R_{1b}, R_{2a} and R_{2b} . Transmitter 1, encodes the message W_1 and uses the SPC with two code-books X_{1a}^n and X_{1b}^n . Transmitter 2, by access to the message W_1 and the channel state S_1^n uses the SPC with two code-books X_{1a}^n and X_{1b}^n . Then, it splits the message W_2 and uses GPC against $X_{1a}^n, X_{1b}^n, S_1^n$ in two steps to create X_2^n . In the first step, transmitter 2 uses binning against $X_{1a}^n, X_{1b}^n, S_1^n$ to create U^n of rate R_{2b} . In the second step, it uses binning against X_{1a}^n, X_{1b}^n and S_1^n conditioned on U^n to create V^n of rate R_{2a} . Finally, it uses $U^n, V^n, X_{1a}^n, X_{1b}^n, S_1^n$ to construct X_2^n . Based on this encoding scheme, we have the following result on the achievable equivocation-rate region.

Theorem 1 (Achievable equivocation-rate region)

The set of equivocation-rates $(R_{1a}, R_{1b}, R_{2a}, R_{2b}, R_{e_2})$ is achievable if it satisfies

$$R_1 \leq I(X_1; Y_1, U|Q), \quad (10)$$

$$R_{1b} \leq I(X_{1b}; Y_1, U|X_{1a}, Q), \quad (11)$$

$$R_{2a} \leq I(V; Y_2, S_2|U, Q) - I(V; X_1, S_1|U, Q), \quad (12)$$

$$R_2 \leq I(V, U; Y_2, S_2|Q) - I(V, U; X_1, S_1|Q), \quad (13)$$

$$R_1 + R_{2b} \leq I(X_1, U; Y_1|Q), \quad (14)$$

$$R_{1b} + R_{2b} \leq I(X_{1b}, U; Y_2|X_{1a}, Q), \quad (15)$$

$$R_{e_2} \leq I(V; Y_2, S_2, U|Q) - I(V, S_1; X_1, Y_1, U|Q), \quad (16)$$

for input distribution factors as

$$p(q)p(x_{1a}, x_{1b}, u, v, x_1, x_2, s_1, s_2|q) \times p(y_1, y_2|x_1, x_2, s_1, s_2), \quad (17)$$

in which the right-hand-sides (r.h.s.) of the equations (10)–(16) are non-negative and Q is a time-sharing random variable.

Proof

See Appendix A. \square

Using the Fourier-Motzkin elimination [16], the following explicit description of the region is derived.

Corollary 1

The set of equivocation-rates (R_1, R_2, R_{e_2}) is achievable if it satisfies

$$R_1 \leq \min\{I(X_1; Y_1, U|Q), I(X_1, U; Y_1|Q)\}, \quad (18)$$

$$R_2 \leq I(V, U; Y_2, S_2|Q) - I(V, U; X_1, S_1|Q), \quad (19)$$

$$R_1 + R_2 \leq I(V; Y_2, S_2|U, Q) - I(V; X_1, S_1|U, Q) + I(X_1, U; Y_1|Q), \quad (20)$$

$$R_{e_2} \leq I(V; Y_2, S_2, U|Q) - I(V, S_1; X_1, Y_1, U|Q), \quad (21)$$

for input distribution factors as (17).

Remark 1

Theorem 1 without secrecy aspect and by substituting $S_1 = S_2 = \emptyset$, is reduced to the result of [6, Theorem 1] for the CIC. Moreover, the equivocation-rate (16), by substituting $S_1 = S_2 = \emptyset$, is reduced to equivocation-rate of [13, Theorem 1]. It means that Theorem 1 includes the results of [6] and [13].

3.1.1. The Symmetric Channel State

The special case $S_1 = S_2 = S$ is of special interest. This case resembles the secret-key agreement scenario [16, 26]. The equivocation-rate (16) in this case is reduced to the following theorem:

Theorem 2

The secrecy-rate (SR) of the CIC, when the state sequence s^n is known at the transmitter and the receiver, is given by

$$R_{e_2}^{SR} \leq I(V; Y_2|U, S) - I(V; X_1, Y_1|U, S) + H(S|U, X_1, Y_1). \quad (22)$$

Proof

The achievability of (22) results from (16) as follows.

$$\begin{aligned} R_{e_2} &\leq I(V; Y_2, S, U) - I(V, S; X_1, Y_1, U) \\ &= I(V; Y_2, U|S) - I(V; X_1, Y_1, U|S) \\ &\quad + I(V; S) - I(S; X_1, Y_1, U) \\ &= I(V; Y_2, U|S) - I(V; X_1, Y_1, U|S) \\ &\quad + H(S|U, X_1, Y_1) - H(S|V) \\ &\leq I(V; Y_2, U|S) - I(V; X_1, Y_1, U|S) \\ &\quad + H(S|U, X_1, Y_1), \end{aligned} \quad (23)$$

in which the last inequality follows from the non-negativity of the entropy function. Note that V is an optimal choice. Therefore, selecting $V = (V, S)$ leads to $H(S|V) = 0$, and the bound in the last inequality will be tight. An alternative proof can be derived directly from the secret-key agreement method taken in [26, Theorem 3]. \square

Remark 2

The inner bound of Theorem 2 can be interpreted from the secret-key agreement point of view [26, Theorem 3]. The term $I(V; Y_2|U, S) - I(V; X_1, Y_1|U, S)$ is the rate of a multiplexed CIC in which the cognitive transmitter and both the receivers (the primary and the secondary receivers), have knowledge of s^n and the common message u^n , non-causally. The second term $H(S|U, X_1, Y_1)$ is the additional secret-key rate which can be produced by using the fact that the channel state s^n is only known to the cognitive transmitter-receiver pair. For more details on using the channel state as a shared secret-key between the transmitter-receiver pair, see [26].

3.2. Outer bounds

The following theorems provide two outer bounds on the capacity region of the CIC-PCSI. In the first outer bound, we use the usual approach taken in the previous work [6, 13] based on the Fano's inequality. In the second outer bound, we use the approach taken by [7], which only depends on the conditional marginal distributions of the channel outputs given the inputs. This outer bound does not include auxiliary random variables and every mutual information term involves the inputs and outputs of the channel. Therefore, the second outer bound is looser than the first one, but can be more easily evaluated.

Theorem 3 (Outer bound 1)

The set of rates (R_1, R_2, R_{e_2}) satisfying

$$R_1 \leq \min\{I(U, V_1; Y_1), I(V_1; Y_1, U)\}, \quad (24)$$

$$R_2 \leq I(U, V_2; Y_2|S_1, S_2), \quad (25)$$

$$\begin{aligned} R_1 + R_2 &\leq \min \left\{ I(V_2; Y_2|U, V_1, S_1, S_2) \right. \\ &\quad + I(V_1, U; Y_1), I(V_2, U; Y_2|S_1, S_2) \\ &\quad \left. + I(V_1; Y_1|U, V_2) \right\}, \end{aligned} \quad (26)$$

$$\begin{aligned} R_{e_2} &\leq \min \left\{ I(V_2; Y_2|U) - I(V_2; Y_1|U), \right. \\ &\quad \left. I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U) \right\}, \end{aligned} \quad (27)$$

for input distribution that factors as

$$p(s_1)p(s_2)p(v_1)p(v_2)p(u|v_1, v_2)p(x_1|v_1) \times p(x_2|u, v_1, v_2, s_1)p(y_1, y_2|x_1, x_2, s_1, s_2), \quad (28)$$

is an outer bound on the capacity of this channel.

Proof

The proof of Theorem 3 is relegated to Appendix B. \square

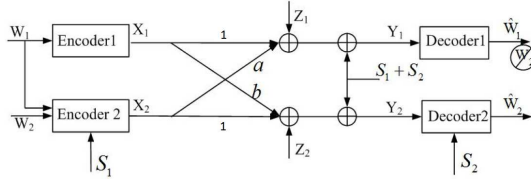


Figure 2: The Gaussian cognitive interference channel with channel state available at the transmitter and the receiver, with a confidential message.

Theorem 4 (Outer bound 2)

The set of rates (R_1, R_2, R_{e2}) satisfying

$$R_1 \leq I(X_1, X_2; Y_1), \quad (29)$$

$$R_2 \leq I(X_2; Y_2 | X_1, S_1, S_2), \quad (30)$$

$$R_1 + R_2 \leq I(Y_1; X_1, X_2, S_1, S_2) + I(X_2; Y_2 | X_1, S_1, S_2, Y_1'), \quad (31)$$

$$R_{e2} \leq \min \left\{ I(X_2; Y_2) - I(X_2; Y_1), I(X_2; Y_2 | X_1) - I(X_2; Y_1 | X_1) \right\}, \quad (32)$$

for all distributions P_{X_1, X_2} and $P_{Y_2, Y_1' | X_1, X_2, S_1, S_2}$, where Y_1' has the same marginal distribution as Y_1 , i. e., $P_{Y_1' | X_1, X_2, S_1, S_2} = P_{Y_1 | X_1, X_2, S_1, S_2}$, is an outer bound on the capacity of this channel.

Outline of the proof

The rates (29)–(31) are derived using the side information approach taken by [7]. The rate (32) is derived according to the previous rate (27) by substituting the auxiliary random variables V_1 and V_2 by X_1 and X_2 , respectively. This outer bound is looser than the one in Theorem 3, but it does not include auxiliary random variables and thus it can be more easily evaluated. The details on the proof are relegated to Appendix C. \square

3.3. The Gaussian example

To clarify our results more perceptibly, consider the Gaussian CIC-PCSI. The channel model is shown in Figure 2, and can be described as follows:

$$\begin{aligned} Y_1 &= X_1 + aX_2 + S_1 + S_2 + Z_1, \\ Y_2 &= bX_1 + X_2 + S_1 + S_2 + Z_2, \end{aligned} \quad (33)$$

where X_i and Y_i denotes the input and the output of the i -th transmitter-receiver pair. $Z_i \sim \mathcal{N}(0, 1)$ is Additive White Gaussian Noise (AWGN) at the i -th receiver where $i \in \{1, 2\}$. $S_i \sim \mathcal{N}(0, K_i)$ denotes the partial channel state sequences which are known at the cognitive transmitter and the corresponding receiver, respectively. The constants a and b are the real-valued channel gains in the interfering links and the average power constraint is $\frac{1}{n} \sum_{k=1}^n (X_{i,k}(t))^2 \leq P_i, i \in \{1, 2\}$. In this model, for simplicity, we consider the partial channel state sequences

to be additive and independent Gaussian random variables. This model can be motivated by the case in which two different interfering signals affect the channel, and each one is estimated at one of the cognitive transmitter-receiver nodes. Now, we consider the cases in which $a \leq 1$ and $a > 1$, separately.

3.3.1. The case $a \leq 1$

This case is reported as the *weak interference* case in the literature [2, 3]. The capacity region of the CIC in this case without CSI is determined by [5, 27], in which the cognitive encoder uses Dirty Paper Coding (DPC) [19] for W_2 against W_1 . Furthermore, using the SPC in the cognitive transmitter, the message W_1 is conveyed to receiver 2. In the weak interference case, receiver 2 does not suffer from the interference, since, transmitter 2 uses DPC on X_2 against X_1 and known channel state. Moreover, the primary receiver is not affected by the interfering signal X_2 due to the weak interference. The following theorem describes the achievable equivocation-rate region of the Gaussian CIC-PCSI in this case.

Theorem 5 (Achievable equivocation-rate region)

The set of rates (R_1, R_2, R_{e2}) satisfying

$$R_1 \leq \mathcal{C}\left(\frac{P_1}{K_2 + 1}\right), \quad (34)$$

$$R_2 \leq \mathcal{C}((1 - \rho^2)P_2), \quad (35)$$

$$R_{e2} \leq \mathcal{C}((1 - \rho^2)P_2) - \mathcal{C}((1 - \rho^2)a^2P_2), \quad (36)$$

in which $\mathcal{C}(x) = \frac{1}{2}(1 + x)$ and $\rho \in [0, 1]$, is an achievable equivocation-rate region of the Gaussian CIC-PCSI, shown in Figure 2 for the case $a \leq 1$.

Proof

The proof is similar to the one presented in [27] without secrecy and by substituting $X_i \sim \mathcal{N}(0, P_i)$ for $i \in \{1, 2\}$ and $E[X_1 X_2] = \rho\sqrt{P_1 P_2}$. The channel state S_1 is treated as interference by the cognitive transmitter in DPC and does not affect the rate. On the other hand, the channel state S_2 , which is known non-causally at the cognitive receiver, can be easily canceled out. Thus, these channel states do not affect the rate (35). The primary receiver 1 is affected by the channel state S_2 as an additional interference, but the channel state S_1 is canceled out for this receiver by the cognitive transmitter's cooperation. For more details on the proof see [27]. \square

Remark 3

The achievable equivocation-rate region for the Gaussian CIC-PCSI in Theorem 5 is maximized for $\rho = 0$ since $a \leq 1$. Thus in this case, the cognitive transmitter meets its capacity and the equivocation leads to $\mathcal{C}(P_2) - \mathcal{C}(a^2 P_2)$.

3.3.2. The case $a > 1$

In this case, which is known as the *strong interference* [2, 3], the channel output at the cognitive receiver is a degraded version of that at the primary one, thus there is no secrecy in this condition, i. e., $R_{e2} = 0$. In this

case, receiver 1, having better observation of X_2 than the cognitive receiver, can decode the message of the cognitive transmitter without any penalty rate. The capacity of the CIC without channel state [2, 27], is a trivial outer bound on the capacity of the CIC-PCSI. This outer bound is presented in the following.

Theorem 6 (Gaussian outer bound [2, Theorem 2])

The set of rates (R_1, R_2) satisfying

$$R_2 \leq \mathcal{C}((1 - \rho^2)P_2), \quad (37)$$

$$R_1 + R_2 \leq \mathcal{C}(P_1 + a^2 P_2 + 2a\rho\sqrt{P_1 P_2}), \quad (38)$$

$$R_1 + R_2 \leq \mathcal{C}(b^2 P_1 + P_2 + 2b\rho\sqrt{P_1 P_2}), \quad (39)$$

is an outer bound on the capacity of the Gaussian CIC-PCSI for the case $a > 1$.

4. USING THE SUPERPOSITION CODING

The cognitive transmitter can superimpose part of its message on X_1^n instead of binning. Thus, it should split its message as $W_2 = W_{21} + W_{22}$, in which W_{21} is intended to both receivers and W_{22} is only decodable at the cognitive receiver. Moreover, the cognitive transmitter uses GPC via three auxiliary random variables T , U and V to reduce the channel state interference for W_1 , W_{21} and W_{22} , respectively. In particular, T deals with state interference for either receiver 1 or receiver 2 to decode W_1 ; U deals with state interference for either receiver 1 or receiver 2 to decode W_{21} ; and V deals with state interference for receiver 2 to decode W_{22} . Now, we propose the main results which are derived based on this scheme.

4.1. An Inner Bound

Theorem 7 (Achievable equivocation-rate region)

The set of rates $(R_1, R_{21}, R_{22}, R_{e2})$ is achievable if it satisfies

$$R_1 + R_{21} \leq I(T, U, X_1; Y_1) - I(T, U; S_1|X_1), \quad (40)$$

$$R_{22} \leq I(V; Y_2, S_2|U, X_1, T) - I(V; S_1|U, X_1, T), \quad (41)$$

$$R_2 \leq I(U, V; Y_2, S_2|X_1, T) - I(U, V; S_1|X_1, T), \quad (42)$$

$$R_2 \leq I(T, U, V; Y_2, S_2|X_1) - I(T, U, V; S_1|X_1), \quad (43)$$

$$R_1 + R_2 \leq I(T, U, V, X_1; Y_2, S_2) - I(T, U, V; S_1|X_1), \quad (44)$$

$$R_{e2} \leq I(V; Y_2, S_2|U, X_1, T) - \max\{I(V; S_1|U, X_1, T), I(V; Y_1|U, X_1, T)\}, \quad (45)$$

for input distribution factors as

$$P_{X_1 S_1 S_2 T U V X_2 Y_1 Y_2} = P_{S_1} P_{S_2} P_{X_1} \times P_{T U V X_2|X_1 S_1} P_{Y_1 Y_2|X_1 X_2 S_1 S_2}, \quad (46)$$

in which the r.h.s. of the equations (40)–(45) are non-negative and T, U, V are auxiliary random variables.

Proof

The proof is relegated to Appendix D. \square

4.1.1. The Symmetric Channel State

For the special case $S_1 = S_2 = S$, we have the following result.

Corollary 2

For the case in which $S_1 = S_2 = S$, the set of rates (R_1, R_2, R_{e2}) is achievable if it satisfies

$$R_1 \leq I(U, X_1; Y_1) - I(U; S|X_1), \quad (47)$$

$$R_2 \leq I(X_2; Y_2|X_1, S) \quad (48)$$

$$R_1 + R_2 \leq I(U, X_1; Y_1) + I(X_2; Y_2|X_1, S) - I(U; S|X_1), \quad (49)$$

$$R_{e2} \leq \min\{I(X_2; Y_2|U, X_1, S), I(X_2; Y_2, S|U, X_1) - I(X_2; Y_1|U, X_1)\}, \quad (50)$$

for input distribution that factors as

$$P_{S X_1 X_2 Y_1 Y_2} = P_S P_{X_1} P_{X_2|X_1 S} P_{Y_1 Y_2|X_1 X_2 S}. \quad (51)$$

Proof

The proof follows directly from Theorem 7, by substituting $T = X_1, V = X_2$ and $S_1 = S_2 = S$. \square

4.2. Outer Bound

Now, we provide an outer bound on the capacity of the CIC-PCSI, as follows.

Theorem 8 (Outer bound 3)

An outer bound on the capacity of the CIC-PCSI consists of the rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(T, U, X_1; Y_1) - I(T, U; S_1|X_1), \quad (52)$$

$$R_2 \leq I(T, V; Y_2, S_2|X_1) - I(T, V; S_1|X_1), \quad (53)$$

$$R_1 + R_2 \leq I(T, V, X_1; Y_2, S_2) - I(T, V; S_1|X_1), \quad (54)$$

for input distribution that factors as

$$P_{X_1 S_1 S_2 T V X_2 Y_1 Y_2} = P_{S_1} P_{S_2} P_{X_1} P_{T V X_2|X_1 S_1} \times P_{Y_1 Y_2|X_1 X_2 S_1 S_2}. \quad (55)$$

Proof

The proof is similar to one taken by [3, Appendix F] by using the Fano's inequality. \square

4.3. The Gaussian Example

In this section, we consider the CIC with partial channel states (shown in Figure 2) with the channel outputs as (33). Similar to the cases considered in Section III-C, when $a > 1$, i. e., *Strong Interference*, we have no secrecy. Thus, we consider the other case $a \leq 1$. We provide the following theorem for the Gaussian CIC-PCSI.

Theorem 9 (Achievable equivocation-rate region)

For the Gaussian CIC-PCSI, in the case that $a \leq 1$, the achievable equivocation-rate region consists of the rate triples (R_1, R_2, R_{e2}) which satisfy (56)–(59), in the above of the page, in which $P_2'' = \rho P_2$ and $0 \leq \rho, \rho_1, \rho_2 \leq 1$.

$$R_1 \leq \mathcal{C}\left(\frac{P_1 + a^2 P_2 + K_1 + K_2 + 1 + 2a\rho_1\sqrt{P_1 P_2} + 2a\rho_2\sqrt{P_2 K_1}}{K_1(a^2 P_2'' + K_2 + 1)}\right), \quad (56)$$

$$R_2 \leq \mathcal{C}(P_2''), \quad (57)$$

$$R_1 + R_2 \leq \mathcal{C}(b^2 P_1 + P_2 + K_1 + 2b\rho_1\sqrt{P_1 P_2} + 2\rho_2\sqrt{P_2 K_1}) - \frac{1}{2} \log(K_1), \quad (58)$$

$$R_{e_2} \leq \mathcal{C}(P_2'') - \mathcal{C}\left(\frac{a^2 P_2''}{K_2 + 1}\right), \quad (59)$$

Proof

The proof is based on Theorem 7, by substituting $T = (U, S_1)$ and $V = X_2$ and choosing the following jointly Gaussian distributions for the random variables:

$$X_1 \sim \mathcal{N}(0, P_1), \quad X_2 \sim \mathcal{N}(0, P_2), \quad (60)$$

$$X_2 = X_2' + X_2'' + \rho_1 \sqrt{\frac{P_2}{P_1}} X_1 + \rho_2 \sqrt{\frac{P_2}{K_1}} S_1, \quad (61)$$

$$X_2' \sim \mathcal{N}(0, P_2'), \quad X_2'' \sim \mathcal{N}(0, P_2''), \quad (62)$$

$$P_2' + P_2'' = (1 - \rho_1^2 - \rho_2^2) P_2, \quad (63)$$

$$U = X_2' + \alpha S_1, \quad (64)$$

in which X_1, X_2', X_2'' , and S_1, S_2 are independent. Transmitter 2, splits its power into three parts: $\rho_1^2 P_2$, which is used for cooperating with the primary transmitter sending W_1 ; $P_2' + \rho_2^2 P_2$, which is used in dirty paper coding to deal with the state at receiver 1 via an auxiliary random variable U ; and P_2'' which is used for transmitting W_2 . The mutual information formulas in (56)-(59) are calculated by the approach taken by [3]. \square

To compare the results of Theorem 9 with the achievable equivocation-rate of Theorem 5, we consider a simple case of Theorem 9 in which the cognitive transmitter uses all its power to send its individual message. For this case we have the following corollary.

Corollary 3 (Perfect Secrecy Condition)

For the Gaussian CIC-PCSI, in the case that $a \leq 1$, the achievable secrecy rate region consists the set of rates (R_1, R_2) which satisfies

$$R_1 \leq \mathcal{C}\left(\frac{P_1 + a^2 P_2 + K_1 + K_2 + 1}{K_1(a^2 P_2 + K_2 + 1)}\right), \quad (65)$$

$$R_2 \leq \mathcal{C}(P_2) - \mathcal{C}\left(\frac{a^2 P_2}{K_2 + 1}\right), \quad (66)$$

$$R_1 + R_2 \leq \mathcal{C}(b^2 P_1 + P_2 + K_1) - \frac{1}{2} \log K_1. \quad (67)$$

Proof

The proof is directly derived from Theorem 9 by considering the perfect secrecy condition in which $R_2 \leq \min\{R_2, R_{e_2}\}$, and by substituting $\rho_1 = \rho_2 = 0$ and $\rho = 1, X_2' = \emptyset$, \square

Remark 4

Comparing the results of Corollary 3 with the achievable equivocation-rate region of Theorem 5 shows that the secrecy rate of (66) is higher than the one of (36), because of $K_2 \geq 0$. It means that the SPC approach achieves higher secrecy rate than the GPC in general case. Moreover, comparing (65) with (34) shows that for the case of $a \leq a^\dagger$, where

$$a^\dagger = \sqrt{\frac{(K_2 + 1)(P_1 + K_1 + K_2 + 1) - P_1 K_1 (K_2 + 1)}{P_1 P_2 K_1 - P_2 (K_2 + 1)}}$$

the SPC approach obtains higher achievable rate for the primary transmitter than the GPC, and for the case of $a > a^\dagger$ vice versa. Thus, in the case of $a > a^\dagger$, there is a trade off between the secrecy rate of the cognitive transmitter and the achievable rate of the primary one. Figure 3 shows the secrecy rate of the cognitive transmitter vs. the achievable rate of the primary one, using the GPC and the SPC approaches, and it illustrates the trade off between the R_2 and R_1 in the case of $a > a^\dagger$.

5. CONCLUSIONS

In this paper we studied the Cognitive Interference Channel in which the partial channel state's information is available non-causally at the cognitive transmitter and corresponding receiver. Furthermore, the cognitive transmitter wishes to keep its message confidential at the primary receiver, in addition to have a reliable communication with its destination. We use the Gel'fand-Pinsker coding (GPC) and the superposition coding (SPC) to show that how the cognitive transmitter can use the side information about the primary message and the channel state sequence to improve its achievable rate and cooperate with the primary one. Therefore, we have derived the achievable equivocation-rate region for this channel in two cases: by using GPC and SPC. Moreover, in each case the outer bounds on the capacity and extension to a simple Gaussian example is presented. In the Gaussian case, we consider a case in which the partial channel state sequences are additive and independent Gaussian random variables, and it is shown that in some cases, there is a trade off between the secrecy rate of the cognitive transmitter and the achievable rate of the primary one, using the GPC

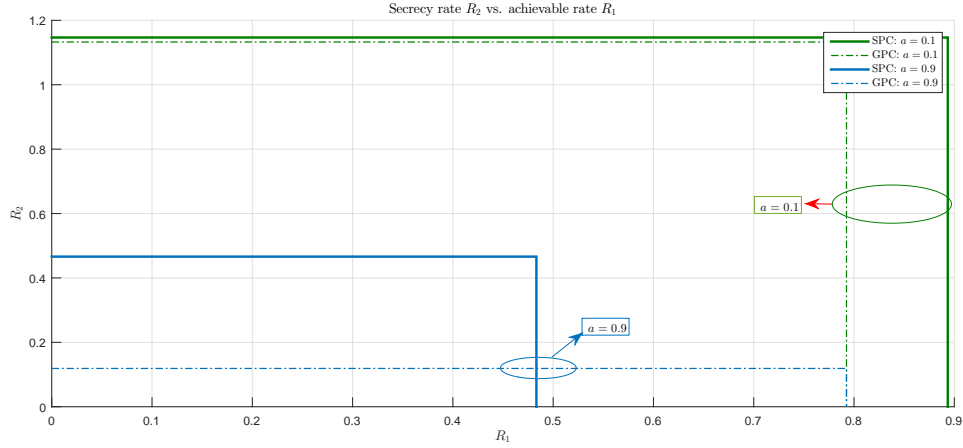


Figure 3: The achievable equivocation-rate region of Theorem 5 (GPC), and the achievable secrecy rate region of Theorem 9 (SPC) for special values $P_1 = 4, P_2 = 4, K_1 = K_2 = 1, b = 0.3$ and $a = 0.1, 0.9$. In this case $a^\dagger = 0.866$, and for $a > a^\dagger$, there is a trade off between the secrecy rate of the cognitive transmitter and the achievable rate of the primary one.

and GPC approaches. Thus, the cognitive transmitter can obtain the desired region by choosing the proper coding scheme.

A. PROOF OF THEOREM 1

Proof

The proof is established on the proof of [6, Theorem 1] and [13, Theorem 1]. After introducing the code-book generation, and the encoding-decoding scheme, the proof of Theorem 1 is presented in two steps. In step I, we prove the reliability of the rate region, i. e., the condition under which the probability of error tends to zero for $n \rightarrow \infty$. This step yields to the equations (10)-(15). In step II, we will calculate the equivocation to evaluate the secrecy level. This step provides the equation (16).

Code-book generation:

1. For split rates (8)-(9), generate $2^{nR_{1a}}$ codewords $x_{1a}^n(w_{1a})$, $w_{1a} \in \{1, 2, \dots, 2^{nR_{1a}}\}$, choosing $x_{1a,n}^n(w_{1a})$ independently according to $P_{X_{1a}}(\cdot)$.
2. For each w_{1a} , generate $2^{nR_{1b}}$ codewords $x_{1b}^n(w_{1a}, w_{1b})$ using $\prod_{i=1}^n P_{X_{1b}|X_{1a}}(\cdot | x_{1a,i}(w_{1a}))$, where $w_{1b} \in \{1, 2, \dots, 2^{nR_{1b}}\}$.
3. Over each pair (w_{1a}, w_{1b}) we generate $x_1^n(w_{1a}, w_{1b})$ where x_1 is a deterministic function of (x_{1a}, x_{1b}) .
4. Generate $2^{n(R_{2b}+R'_{2b})}$ codewords $u^n(w_{2b}, b_{2b})$, $w_{2b} \in \{1, 2, \dots, 2^{nR_{2b}}\}$, $b_{2b} \in \{1, 2, \dots, 2^{nR'_{2b}}\}$ using $P_U(\cdot)$.
5. For each $u^n(w_{2b}, b_{2b})$ generate $2^{n(R_{2a}+R'_{2a})}$ codewords $v^n(w_{2b}, b_{2b}, w_{2a}, b_{2a})$, $w_{2a} \in$

$\{1, 2, \dots, 2^{nR_{2a}}\}$, $b_{2a} \in \{1, 2, \dots, 2^{nR'_{2a}}\}$ using $\prod_{n=1}^n P_{V|U}(\cdot | u_n(w_{2b}, b_{2b}))$.

6. Now, define $L_1 = I(V; Y_2, S_2|U) - I(V; Y_1, X_1|U)$, $L_2 = I(V; Y_1, X_1|U)$. Note that, here we assume that $R_{2a} > L_1 \geq 0$, for the case $R_{2a} < L_1$ the similar coding scheme can be used to obtain the *perfect secrecy*, which is mentioned at the end of the proof. Let

$$\mathcal{W}_{2a} = \mathcal{A} \times \mathcal{B} \quad (68)$$

where $\mathcal{A} = \{1, 2, \dots, 2^{n(R_{2a}-L_1)}\}$ and $\mathcal{B} = \{1, 2, \dots, 2^{nL_1}\}$. Then, we define the mapping $f: \mathcal{B} \rightarrow \mathcal{C}$ to partition \mathcal{B} into 2^{nL_1} subsets with nearly equal size which means

$$\|f^{-1}(c_1)\| \leq 2\|f^{-1}(c_2)\| \text{ for each } c_1, c_2 \in \mathcal{C}. \quad (69)$$

Now we define the mapping $w_{2a} = (a, c) \rightarrow (a, b)$, in which b is chosen randomly from the set $f^{-1}(c) \subset \mathcal{B}$.

7. Over each pair w_1 and $w_2(w_{2a}(a, c), w_{2b})$, we generate x_1^n and $x_2^n(w_1, w_{2b}, w_{2a}(a, c), b_{2b}, b_{2a}, s_1)$ where x_2 is a deterministic function of (u, v, x_1, s_1) .

Encoding:

1. Encoder 2 splits the nR_2 bits w_2 into nR_{2a} bits w_{2a} and nR_{2b} bits w_{2b} . Similarly, it splits the nR_1 bits w_1 into nR_{1a} bits w_{1a} and nR_{1b} bits w_{1b} . Thus,

$$w_2 = (w_{2a}, w_{2b}), \quad w_1 = (w_{1a}, w_{1b}). \quad (70)$$

2. Encoder 2, finds a bin index b_{2b} such that $(u^n(w_{2b}, b_{2b}), x_{1a}^n(w_{1a}), x_{1b}^n(w_{1a}, w_{1b}), s_1^n)$

are jointly typical. If such a b_{2b} is not found, it chooses $b_{2b} = 1$.

3. For each (w_{2b}, b_{2b}) and given s_1^n encoder 2 finds a bin index b_{2a} such that $(v^n(w_{2b}, b_{2b}, w_{2a}, b_{2a}), u^n(w_{2b}, b_{2b}), x_{1a}^n(w_{1a}), x_{1b}^n(w_{1a}, w_{1b}), s_1^n)$ are jointly typical.
4. Transmitter 1 transmits $x_1^n(w_{1a}, w_{1b})$.
5. Transmitter 2 transmits $x_2^n(w_{1a}, w_{1b}, w_{2a}, b_{2a}, w_{2b}, b_{2b}, s_1^n)$.

Decoding:

1. For given y_1^n , decoder 1 chooses $(\hat{w}_{1a}, \hat{w}_{1b}, \hat{w}_{2b}, \hat{b}_{2b})$ such that $(u^n(\hat{w}_{2b}, \hat{b}_{2b}), x_{1a}^n(\hat{w}_{1a}), x_{1b}^n(\hat{w}_{1a}, \hat{w}_{1b}), y_1^n)$ are jointly typical. If there is no such quadruple it chooses $(1, 1, 1, 1)$.
2. For given y_2^n , s_2^n decoder 2 chooses $(\hat{w}_{2b}, \hat{b}_{2b}, \hat{w}_{2a}, \hat{b}_{2a})$ such that $(v^n(\hat{w}_{2b}, \hat{b}_{2b}, \hat{w}_{2a}, \hat{b}_{2a}), u^n(\hat{w}_{2b}, \hat{b}_{2b}), y_2^n, s_2^n)$ are jointly typical. If there are more than one such quadruple, it chooses one of them. If there is not any quadruple, it chooses $(1, 1, 1, 1)$.

A.1. Step I: (Reliability) achievability of the rate region (10)–(15)

Reliability of the rate region (10)–(15) will be proved here by analyzing the error probability.

Error analysis: Using this scheme for coding and decoding, analysis of the error is derived following [6]. First, we suppose that $(w_{2a}, w_{2b}, w_{1a}, w_{1b}) = (1, 1, 1, 1)$ is sent. An encoder error occurs in one of the following situations.

- 1- \mathcal{E}_1 : Encoder 2, cannot find a bin index b_{2b} such that $(u^n(1, b_{2b}), x_{1a}^n(1), x_{1b}^n(1, 1), s_1^n) \in T_{\epsilon}^{(n)}(P_{U, X_{1a}, X_{1b}, S_1})$ in which $T_{\epsilon}^{(n)}(P_{XY})$ denotes the jointly ϵ -typical set with respect to P_{XY} . It can be shown, by covering lemma [16], that for $n \rightarrow \infty$ such b_{2b} exists with high probability if we have

$$R'_{2b} > I(U; X_{1a}, X_{1b}, S_1) + \delta, \quad (71)$$

in which δ tends to zero as $n \rightarrow \infty$ [6].

- 2- \mathcal{E}_2 : After finding $b_{2b} = 1$, encoder 2 cannot find b_{2a} such that $(v^n(1, 1, b_{2a}), u^n(1, 1), x_{1a}^n(1), x_{1b}^n(1, 1), s_1^n) \in T_{\epsilon}^{(n)}(P_{U, V, X_{1a}, X_{1b}, S_1})$. It can be shown [6] that for $n \rightarrow \infty$, such b_{2a} exists with high probability if we have

$$R'_{2a} > I(V; X_{1a}, X_{1b}, S_1 | U) + \delta. \quad (72)$$

Now, we should compute the probabilities of the error events at the decoder, which are shown in TABLE I. The second column of the table shows the corresponding bounds of the rates, which can be shown, make the error probability of each event tend to zero, as $n \rightarrow \infty$. For more details about the derivation of the bounds proposed

in TABLE I see [6]. Using these bounds, the achievability of (10)–(15) are proved.

A.2. Step II: (Security) achievability of the equivocation-rate region (16)

In this step, the achievability of the equivocation-rate region (16) will be driven. To this purpose, we compute the equivocation.

Equivocation-rate calculation: To prove (16), for the equivocation-rate R_{e2} , we follow the proof reported in [2, 13, 28]. We establish computing of the equivocation for the cognitive transmitter as follows.

$$\begin{aligned} & H(W_{2a}, W_{2b} | Y_1^n) \\ & \geq H(W_{2a}, W_{2b} | Y_1^n, W_1, W_{2b}) \\ & = H(W_{2a}, Y_1^n | W_1, W_{2b}) - H(Y_1^n | W_1, W_{2b}) \\ & = H(W_{2a}, Y_1^n, V^n | W_1, W_{2b}) \\ & \quad - H(V^n | W_{2a}, W_1, W_{2b}, Y_1^n) - H(Y_1^n | W_1, W_{2b}) \\ & = H(W_{2a}, V^n | W_1, W_{2b}) \\ & \quad + H(Y_1^n | W_1, W_{2b}, W_{2a}, V^n) \\ & \quad - H(V^n | W_{2a}, W_1, W_{2b}, Y_1^n) - H(Y_1^n | W_1, W_{1b}) \\ & \stackrel{(a)}{\geq} H(V^n | W_1, W_{2b}) + H(Y_1^n | V^n, U^n, X_1^n) \\ & \quad - H(V^n | W_{2a}, W_1, W_{2b}, Y_1^n) - H(Y_1^n | W_1, W_{2b}) \end{aligned} \quad (73)$$

where (a) is because of the fact that given V^n , W_{2a} is uniquely determined and Y_1^n is independent of (W_1, W_{2b}, W_{2a}) given (V^n, U^n, X_1^n) . Now, we bound each term in r.h.s. of (73). For the first term in (73), we have

$$\begin{aligned} & H(V^n | W_1, W_{2b}) \\ & \stackrel{(b)}{\geq} H(V^n | U^n, X_1^n) \\ & \geq H(V^n | U^n, X_1^n) - H(V^n | U^n, Y_2^n, S_2^n) \\ & = I(V^n; Y_2^n, S_2^n | U^n) - I(V^n; X_1^n | U^n) \\ & \stackrel{(c)}{\geq} n[I(V; Y_2, S_2 | U) - I(V; X_1 | U)] \end{aligned} \quad (74)$$

where (b) is derived by using the data processing inequality [29], which implies that V^n is independent of (W_1, W_{2b}) given (U^n, X_1^n) , and (c) is derived using the approach taken in [30, Lemma 3]. For the second term in the r.h.s of (73) we follow the related equations in [2] and obtain

$$\frac{1}{n} H(Y_1^n | V^n, U^n, X_1^n) \geq H(Y_1 | V, U, X_1, S_1) - \epsilon_1, \quad (75)$$

where ϵ_1 is negligible for $n \rightarrow \infty$. To compute the third term in the r.h.s of (73), similar to [2, Lemma 2], by using Fano's inequality we obtain

$$\frac{1}{n} H(V^n | W_{2a}, W_1, W_{2b}, Y_1^n) < \epsilon_2 \quad (76)$$

Table I: Error events in joint decoding and corresponding rate bounds

	Error event	Arbitrarily small positive error probability if
E_1	$(\hat{w}_{2b} \neq 1, \hat{w}_{2a} = 1)$	$R_{2b} + R_{2b} \leq I(U, V; Y_2, S_2)$
E_2	$(\hat{w}_{2b} = 1, \hat{w}_{2a} \neq 1)$	$R_{2a} + R_{2a} \leq I(V; Y_2, S_2 U)$
E_3	$(\hat{w}_{2b} \neq 1, \hat{w}_{2a} \neq 1)$	$R_{2b} + R_{2b} + R_{2a} + R_{2a} \leq I(U, V; Y_2, S_2)$
E'_1	$(\hat{w}_{1a} \neq 1, \hat{w}_{1b} = 1, \hat{w}_{2b} = 1)$	$R_{1a} \leq I(X_{1a}, X_{1b}; U, Y_1)$
E'_2	$(\hat{w}_{1a} \neq 1, \hat{w}_{1b} \neq 1, \hat{w}_{2b} = 1)$	$R_{1a} + R_{1b} \leq I(X_{1a}, X_{1b}; U, Y_1)$
E'_3	$(\hat{w}_{1a} \neq 1, \hat{w}_{1b} = 1, \hat{w}_{2b} \neq 1)$	$R_{1a} + R_{1b} + R_{1b} \leq I(U, X_{1a}, X_{1b}; Y_1) + I(U; X_{1a}, X_{1b})$
E'_4	$(\hat{w}_{1a} \neq 1, \hat{w}_{1b} \neq 1, \hat{w}_{2b} \neq 1)$	$R_{1a} + R_{1b} + R_{2b} + R_{2b} \leq I(U, X_{1a}, X_{1b}; Y_1) + I(U; X_{1a}, X_{1b})$
E'_5	$(\hat{w}_{1a} = 1, \hat{w}_{1b} \neq 1, \hat{w}_{2b} = 1)$	$R_{1b} \leq I(X_{1b}; Y_1, U X_{1a})$
E'_6	$(\hat{w}_{1a} = 1, \hat{w}_{1b} \neq 1, \hat{w}_{2b} \neq 1)$	$R_{1b} + R_{2b} + R_{2b} \leq I(X_{1b}, U; Y_1 X_{1a}) + I(U; X_{1a}, X_{1b})$

where ϵ_2 is negligible, when $n \rightarrow \infty$. To compute the fourth term in (73), first we define

$$\hat{y}_1^n = \begin{cases} y_1^n & \text{if } (u^n(w_{2b}, b_{2b}), x_{1a}^n(w_{1a}), \\ & x_{1b}^n(w_{1a}, w_{1b}), y_1^n) \in T_{\epsilon}^{(n)}(P_{U X_1 Y_1}) \\ z^n & \text{Otherwise} \end{cases} \quad (77)$$

where z^n is an arbitrary sequence that is contained in \mathcal{Y}_1^n . Now, we have

$$\begin{aligned} & \frac{1}{n} H(Y_1^n | W_1, W_{2b}) \\ &= \frac{1}{n} \sum_{w_1, w_{2b}} [Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad H(Y_1^n | W_1 = w_1, W_{2b} = w_{2b})] \\ &\leq \frac{1}{n} \sum_{w_1, w_{2b}} [Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad H(\hat{Y}_1^n, Y_1^n | W_1 = w_1, W_{2b} = w_{2b})] \\ &= \frac{1}{n} \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad \left[H(\hat{Y}_1^n | W_1 = w_1, W_{2b} = w_{2b}) \right. \\ & \quad \left. + H(Y_1^n | W_1 = w_1, W_{2b} = w_{2b}, \hat{Y}_1^n) \right] \quad (78) \end{aligned}$$

For the first term in (78) we can write

$$\begin{aligned} & \frac{1}{n} \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad H(\hat{Y}_1^n | W_1 = w_1, W_{2b} = w_{2b}) \\ &\stackrel{(d)}{\leq} \frac{1}{n} \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad \times \log |T_{\epsilon}^{(n)}(P_{Y_1|U, X_1})| \\ &\leq \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad \times [H(Y_1 | U, X_1) + \epsilon_3] \\ &\leq H(Y_1 | U, X_1) + \epsilon_3, \quad (79) \end{aligned}$$

where (d) is based on AEP [29], and ϵ_3 is negligible for $n \rightarrow \infty$. To bound the second term in the r.h.s of (78), we use Fano's inequality and obtain

$$\begin{aligned} & \frac{1}{n} \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad H(Y_1^n | W_1 = w_1, W_{2b} = w_{2b}, \hat{Y}_1^n) \\ &\leq \frac{1}{n} \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad \left(1 + Pr\{Y_1^n \neq \hat{Y}_1^n | W_1 = w_1, W_{2b} = w_{2b}\} \right. \\ & \quad \left. \times \log |\mathcal{Y}_1|^n \right) \\ &= \frac{1}{n} + \log |\mathcal{Y}_1| \sum_{w_1, w_{2b}} Pr\{W_1 = w_1, W_{2b} = w_{2b}\} \\ & \quad Pr\{Y_1^n \neq \hat{Y}_1^n | W_1 = w_1, W_{2b} = w_{2b}\} \\ &\leq \epsilon_4, \quad (80) \end{aligned}$$

where ϵ_4 is negligible for $n \rightarrow \infty$. Hence, from (79) and (80), the forth term of the r.h.s. of (73) is bounded as

$$\frac{1}{n} H(Y_1^n | W_1, W_{2b}) \leq H(Y_1 | U, X_1) + \epsilon_5, \quad (81)$$

in which ϵ_5 tends to zero for $n \rightarrow \infty$. Substituting (74), (75), (76) and (81) into (73), we obtain

$$\begin{aligned} & \frac{1}{n} H(W_{2a}, W_{2b} | Y_1^n) \\ &\geq I(V; Y_2, S_2, U) - I(V; X_1, U) \\ & \quad + H(Y_1 | V, U, X_1, S_1) - H(Y_1 | U, X_1) - \epsilon_6 \\ &\geq I(V; Y_2, S_2, U) - I(V, S_1; X_1, U) \\ & \quad - I(Y_1; V, S_1 | U, X_1) - \epsilon_6 \\ &= I(V; Y_2, S_2, U) - I(V, S_1; X_1, Y_1, U) - \epsilon_6 \quad (82) \end{aligned}$$

where ϵ_6 is negligible for $n \rightarrow \infty$. Regard to the definition of R_{e2} in (5)-(6) we conclude

$$R_{e2} \leq I(V; Y_2, S_2, U) - I(V, S_1; X_1, Y_1, U). \quad (83)$$

and therefore (16) is proved. \square

B. PROOF OF THEOREM 3

Proof of Theorem 3

For a quadruple code (M_1, M_2, n, P_e) for the CIC-PCSI, we consider the outer bound on R_1 proposed in (24). Using the Fano's inequality we have

$$\begin{aligned} nR_1 &\leq I(W_1; Y_1^n) \\ &= \sum_{i=1}^n I(W_1; Y_{1,i} | Y_{1,i+1}^n) \\ &\leq \sum_{i=1}^n I(W_1, Y_2^{i-1}, Y_{1,i+1}^n; Y_{1,i}) \\ &\stackrel{(e)}{=} \sum_{i=1}^n I(W_1, U_i; Y_{1,i}), \end{aligned} \quad (84)$$

where (e) is derived by substituting $U_i = (Y_2^{i-1}, Y_{1,i+1}^n)$. Then, by substituting $V_{1,i} = W_1$, the outer bound on R_1 is derived. Similarly, we have

$$\begin{aligned} nR_1 &\leq I(W_1; Y_1^n) \\ &\leq \sum_{i=1}^n I(W_1; Y_2^{i-1}, Y_{1,i+1}^n, Y_{1,i}) \\ &\stackrel{(f)}{=} \sum_{i=1}^n I(W_1; Y_{1,i}, U_i), \end{aligned} \quad (85)$$

where (f) is derived by substituting $U_i = (Y_2^{i-1}, Y_{1,i+1}^n)$. Thus, the outer bound on R_1 is proved. The outer bound for R_2 is derived as follows:

$$\begin{aligned} nR_2 &\leq I(W_2; Y_2^n | S_1^n, S_2^n) \\ &= \sum_{i=1}^n I(W_2, Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}, S_1^n, S_2^n) \\ &\quad - I(Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}, S_1^n, S_2^n, W_2) \\ &= \sum_{i=1}^n I(W_2; Y_{2,i} | Y_2^{i-1}, Y_{1,i+1}^n, S_1^n, S_2^n) \\ &\quad + I(Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}, S_1^n, S_2^n) \\ &\quad - I(Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}, S_1^n, S_2^n, W_2) \\ &\stackrel{(g)}{=} \sum_{i=1}^n I(W_2; Y_{2,i} | Y_2^{i-1}, Y_{1,i+1}^n, S_1^n, S_2^n) \\ &\quad + I(Y_2^{i-1}; Y_{1,i}, W_2 | Y_{1,i+1}^n, S_1^n, S_2^n) \\ &\quad - I(W_2; Y_2^{i-1} | Y_{1,i+1}^n, Y_{1,i}, S_1^n, S_2^n) \\ &\quad - I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n, S_1^n, S_2^n, W_2) \end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^n I(W_2; Y_{2,i} | Y_{1,i+1}^n, S_1^n, S_2^n) \\ &\quad - I(W_2; Y_2^{i-1} | Y_{1,i}^n, S_1^n, S_2^n) \\ &\leq \sum_{i=1}^n I(W_2; Y_{2,i} | Y_{1,i+1}^n, S_1^n, S_2^n) \\ &= \sum_{i=1}^n I(W_2, U_i; Y_{2,i} | S_1^n, S_2^n), \end{aligned} \quad (86)$$

where (g) is derived by Csiszár sum identity [16]. Then, by substituting $V_{1,i} = W_1$ and $V_{2,i} = W_2$, the outer bound on R_2 is derived. From Fano's inequality [29, Chapter 7] we have

$$\begin{aligned} &n(R_1 + R_2) \\ &\leq I(W_1; Y_1^n) + I(W_2; Y_2^n | S_1^n, S_2^n) \\ &\stackrel{(h)}{\leq} I(W_1; Y_1^n) + I(W_2; Y_2^n | W_1, S_1^n, S_2^n) \\ &= \sum_{i=1}^n I(W_1; Y_{1,i} | Y_{1,i+1}^n) \\ &\quad + I(W_2; Y_{2,i} | W_1, Y_{1,i+1}^n, S_1^n, S_2^n) \\ &\quad - [I(W_2, Y_{1,i}; Y_2^{i-1} | W_1, Y_{1,i}^n) \\ &\quad - I(Y_{1,i}; Y_2^{i-1} | W_1, Y_{1,i}^n)] \\ &\stackrel{(i)}{\leq} \sum_{i=1}^n I(W_1, Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n) \\ &\quad + I(W_2; Y_{2,i} | W_1, S_1^n, S_2^n, U_i) \\ &\quad - I(Y_{1,i}; Y_2^{i-1} | W_2, W_1, Y_{1,i+1}^n) \\ &\leq I(W_1, U_i; Y_{1,i}) \\ &\quad + I(W_2; Y_{2,i} | W_1, S_1^n, S_2^n, U_i), \end{aligned} \quad (87)$$

where (h) is since that W_2 is independent of W_1 and (i) is derived by substituting $U_i = (Y_2^{i-1}, Y_{1,i+1}^n)$. Similarly, we have

$$\begin{aligned} &n(R_1 + R_2) \\ &\leq I(W_1; Y_1^n | W_2) + I(W_2; Y_2^n | S_1^n, S_2^n) \\ &\stackrel{(j)}{\leq} \sum_{i=1}^n I(W_1; Y_{1,i} | U_i, W_2) + I(W_2, U_i; Y_{2,i} | S_1^n, S_2^n), \end{aligned} \quad (88)$$

and (j) is derived by using the same approach as (87). Finally, for the equivocation-rate region R_{e2} , we derive the outer bound, using the approach taken in [13], as follows:

$$\begin{aligned} nR_{e2} &\leq H(W_2 | Y_1^n) \\ &= H(W_2) - I(W_2; Y_1^n) \\ &= I(W_2; Y_2^n) - I(W_2; Y_1^n) + H(W_2 | Y_2^n) \\ &\stackrel{(k)}{\leq} I(W_2; Y_2^n) - I(W_2; Y_1^n) + 2n\epsilon_n, \end{aligned} \quad (89)$$

where (k) is derived from the Channel Coding Theorem [29, Chapter 7] which implies that in a reliable communication, the entropy of W_2 given Y_2^n is less than ϵ_n

which is negligible as $n \rightarrow \infty$. Then, we have

$$\begin{aligned} I(W_2; Y_1^n) &= \sum_{i=1}^n I(W_2; Y_{1,i} | Y_{1,i+1}^n) \\ &= \sum_{i=1}^n I(W_2; Y_{1,i} | Y_2^{i-1}, Y_{1,i+1}^n) \\ &\quad + I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n) \\ &\quad - I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n, W_2). \end{aligned} \quad (90)$$

Therefore, for (89) we have

$$\begin{aligned} nR_{e2} &\leq \sum_{i=1}^n \left[I(W_2, Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}) \right. \\ &\quad \left. - I(Y_{1,i+1}^n; Y_{2,i} | Y_2^{i-1}, W_2) \right] \\ &\quad - \sum_{i=1}^n I(W_2; Y_{1,i} | Y_2^{i-1}, Y_{1,i+1}^n) \\ &\quad - I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n) \\ &\quad + I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n, W_2) \\ &\stackrel{(l)}{\leq} \sum_{i=1}^n I(W_2; Y_{2,i} | Y_2^{i-1}, Y_{1,i+1}^n) \\ &\quad - I(W_2; Y_{1,i} | Y_2^{i-1}, Y_{1,i+1}^n), \end{aligned} \quad (91)$$

where (l) is derived from the Csiszár sum identity [16] which implies that $\sum_{i=1}^n I(Y_2^{i-1}; Y_{1,i} | Y_{1,i+1}^n, W_2) = \sum_{i=1}^n I(Y_{1,i+1}^n; Y_{2,i} | Y_{2,i-1}^n, W_2)$, and the non-negativity of the mutual information function. Similarly, it can be shown that

$$\begin{aligned} nR_{e2} &\leq \sum_{i=1}^n I(W_2; Y_{2,i} | Y_2^{i-1}, Y_{1,i+1}^n, W_1) \\ &\quad - I(W_2; Y_{1,i} | Y_2^{i-1}, Y_{1,i+1}^n, W_1). \end{aligned} \quad (92)$$

Now, by substituting $U_i = (Y_2^{i-1}, Y_{1,i+1}^n)$, $V_{1,i} = W_1$, $V_{2,i} = W_2$, the proof is completed. \square

C. PROOF OF THEOREM 4

Proof of Theorem 4

For R_1 , using Fano's inequality we have

$$\begin{aligned} nR_1 &\leq I(W_1; Y_1^n) \\ &\leq I(W_1, W_2; Y_1^n) \\ &\leq H(Y_1^n) - H(Y_1^n | W_1, W_2) \\ &\leq H(Y_1^n) - H(Y_1^n | W_1, W_2, X_1^n, X_2^n) \\ &\stackrel{(m)}{\leq} H(Y_1^n) - H(Y_1^n | X_1^n, X_2^n) \\ &\leq I(X_1^n, X_2^n; Y_1^n), \end{aligned} \quad (93)$$

where (m) is due to the fact that Y_1^n is independent of (W_1, W_2) given (X_1^n, X_2^n) . Now, from Fano's

inequality we have

$$\begin{aligned} nR_2 &\leq I(W_2; Y_2^n | S_1^n, S_2^n) \\ &\leq I(W_2; Y_2^n | W_1, S_1^n, S_2^n) \\ &\leq I(W_2, X_2^n; Y_2^n | W_1, X_1^n(W_1), S_1^n, S_2^n) \\ &= H(Y_2^n | W_1, X_1^n, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | W_1, W_2, X_1^n, X_2^n, S_1^n, S_2^n) \\ &\stackrel{(n)}{\leq} H(Y_2^n | X_1^n, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | X_1^n, X_2^n, S_1^n, S_2^n) \\ &= I(X_2^n; Y_2^n | X_1^n, S_1^n, S_2^n), \end{aligned} \quad (94)$$

where (n) is because of the fact that conditioning does not increase the entropy function and Y_2^n is independent of (W_1, W_2) given $(X_1^n, X_2^n, S_1^n, S_2^n)$. Now, for $R_1 + R_2$, from Fano's inequality we have

$$\begin{aligned} n(R_1 + R_2) &\leq I(W_2; Y_2^n | S_1^n, S_2^n) + I(W_1; Y_1^n) \\ &\leq I(W_2; Y_2^n | W_1, S_1^n, S_2^n) + I(W_1; Y_1^n) \\ &\leq I(W_2; Y_2^n, Y_1^n | W_1, S_1^n, S_2^n) + I(W_1; Y_1^n) \\ &\leq I(W_2; Y_1'^n | W_1, S_1^n, S_2^n) \\ &\quad + I(W_2; Y_2^n | Y_1'^n, W_1, S_1^n, S_2^n) + I(W_1; Y_1^n) \\ &= H(Y_1'^n | W_1, S_1^n, S_2^n) - H(Y_1'^n | W_1, W_2, S_1^n, S_2^n) \\ &\quad + H(Y_2^n | Y_1'^n, W_1, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | Y_1'^n, W_1, W_2, S_1^n, S_2^n) + H(Y_1^n) \\ &\quad - H(Y_1^n | W_1) \\ &\stackrel{(o)}{\leq} -H(Y_1'^n | W_1, W_2, S_1^n, S_2^n) \\ &\quad + H(Y_2^n | Y_1'^n, W_1, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | Y_1'^n, W_1, W_2, S_1^n, S_2^n) + H(Y_1^n) \\ &\stackrel{(p)}{\leq} -H(Y_1'^n | W_1, W_2, X_1, X_2, S_1^n, S_2^n) \\ &\quad + H(Y_2^n | Y_1'^n, W_1, X_1, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | Y_1'^n, W_1, W_2, X_1, X_2, S_1^n, S_2^n) + H(Y_1^n) \\ &\leq -H(Y_1'^n | X_1^n, X_2^n, S_1^n, S_2^n) \\ &\quad + H(Y_2^n | Y_1'^n, X_1^n, S_1^n, S_2^n) \\ &\quad - H(Y_2^n | Y_1'^n, X_1^n, X_2^n, S_1^n, S_2^n) + H(Y_1^n) \\ &\leq I(Y_1^n; X_1^n, X_2^n, S_1^n, S_2^n) \\ &\quad + I(Y_2^n; X_2^n | Y_1'^n, X_1^n, S_1^n, S_2^n), \end{aligned} \quad (95)$$

where (o) is because that $H(Y_1'^n | W_1, S_1^n, S_2^n) - H(Y_1^n | W_1) \leq 0$, and (p) is due to the fact that the conditioning does not increase the entropy. Thus, the proof is completed. \square

D. PROOF OF THEOREM 7

Proof of Theorem 7

To derive the equivocation-rate region (40)–(45), first we should propose the code-book generation and the encoding-decoding schemes.

Code-book generation:

1. Generate 2^{nR_1} codewords $x_1^n(w_1), w_1 \in \{1, 2, \dots, 2^{nR_1}\}$, choosing $x_1^n(w_1)$ independently according to $P_{X_1}(\cdot)$.
2. For each $x_1^n(w_1)$, generate $2^{n\tilde{R}_1}$ codewords $t^n(w_1, v_1)$ using $\prod_{i=1}^n P_{T|X_1}(\cdot|x_1^n(w_1))$, where $v_1 \in \{1, 2, \dots, 2^{n\tilde{R}_1}\}$.
3. For each $x_1^n(w_1)$ and $t^n(w_1, v_1)$, generate $u^n(w_1, v_1, w_{21}, v_{21})$ with i.i.d components based on $P_{U|X_1T}$, in which $w_{21} \in \{1, 2, \dots, 2^{nR_{21}}\}$ and $v_{21} \in \{1, 2, \dots, 2^{n\tilde{R}_{21}}\}$.
4. For each $x_1^n(w_1)$, $t^n(w_1, v_1)$ and $u^n(w_1, v_1, w_{21}, v_{21})$ generate $v^n(w_1, v_1, w_{21}, v_{21}, w_{22}, v_{22})$ with i.i.d components based on $P_{V|X_1TU}$, in which $w_{22} \in \{1, 2, \dots, 2^{nR_{22}}\}$ and $v_{22} \in \{1, 2, \dots, 2^{n\tilde{R}_{22}}\}$.
5. Now, distribute v^n sequences randomly to 2^{nR} bin such that each bin contains 2^{nM} sequences, where $R = R_{22} - M$ and $M = \max\{I(V; S_1|U, X_1, T), I(V; Y_1|U, X_1, T)\}$. Then, index each bin by $j \in \{1, 2, \dots, 2^{nR}\}$. Next, partition 2^{nM} sequences in every bin into $2^{n[M-I(V; Y_1|U, X_1, T)]}$ subbin each subbin contains $2^{nI(V; Y_1|U, X_1, T)}$ sequences. Index each subbin by $a \in \{1, 2, \dots, 2^{n[M-I(V; Y_1|U, X_1, T)]}\}$ and let A be the random variable to represent the index of the subbin, and let B be the random variable to represent the index of the sequences in each subbin.

Encoding: Define $\mathcal{A} = 1, 2, \dots, A$ and $\mathcal{B} = 1, 2, \dots, B$ where A and B are defined before. Let $\mathcal{W}_{22} = \mathcal{A} \times \mathcal{C}$ where $\mathcal{C} = \{1, 2, \dots, B\}$. Now, define the mapping $g: \mathcal{B} \rightarrow \mathcal{C}$ to map \mathcal{B} into \mathcal{C} subsets with nearly equal size. Encoder 1 for given w_1 , transmits $x_1^n(w_1)$. Encoder 2 for given $w_1, x_1^n(w_1)$ and s_1^n , chooses $t^n(w_1, v_1)$ such that $(t^n(w_1, v_1), x_1^n(w_1), s_1^n) \in T_{\epsilon}^{(n)}(P_{T, X_1, S_1})$. For given w_{21} and $t^n(w_1, v_1)$ it chooses $u^n(w_1, v_1, w_{21}, v_{21})$ such that $(u^n, t^n, x_1^n, s_1^n) \in T_{\epsilon}^{(n)}(P_{U, T, X_1, S_1})$. Next, for given w_{22} , it uses the mapping $w_{22} = (a, c) \rightarrow (a, b)$ which b is chosen randomly from the set $g^{-1}(c) \subset \mathcal{B}$. Then, it chooses $v^n(w_1, v_1, w_{21}, v_{21}, w_{22}(a, b), v_{22})$ such that $(v^n, u^n, t^n, x_1^n, s_1^n) \in T_{\epsilon}^{(n)}(P_{V, U, T, X_1, S_1})$. Finally, it transmits $x_2^n(v^n, u^n, t^n, x_1^n, s_1^n)$.

Decoding: Decoder 1, given y_1^n , finds $(\hat{w}_1, \hat{v}_1, \hat{w}_{21}, \hat{v}_{21})$ such that $(u^n(\hat{w}_1, \hat{v}_1, \hat{w}_{21}, \hat{v}_{21}), t^n(\hat{w}_1, \hat{v}_1), x_1^n(\hat{w}_1), s_2^n) \in T_{\epsilon}^{(n)}(P_{U, T, X_1, S_2})$. Decoder 2, given y_2^n and s_2^n , finds $(\hat{w}_1, \hat{v}_1, \hat{w}_{21}, \hat{v}_{21}, \hat{w}_{22}(a, b), \hat{v}_{22})$ such that

$$(v^n(\hat{w}_1, \hat{v}_1, \hat{w}_{21}, \hat{v}_{21}, \hat{w}_{22}(a, b), \hat{v}_{22}), u^n(\hat{w}_1, \hat{v}_1, \hat{w}_{21}, \hat{v}_{21}), t^n(\hat{w}_1, \hat{v}_1), x_1^n(\hat{w}_1), s_2^n) \in T_{\epsilon}^{(n)}(P_{V, U, T, X_1, S_2}).$$

Error analysis: First, fix the channel joint distribution as (55). The error analysis is similar to the one presented in [3]. Thus, the equations (40)–(44) are derived by combining these results.

Equivocation-rate calculation: The equivocation of the W_2 at receiver 1 is calculated as follows:

$$\begin{aligned} & H(W_2|Y_1^n) \\ &= H(W_2, Y_1^n) - H(Y_1^n) \\ &= H(W_2, Y_1^n, A, W_1) - H(Y_1^n) - H(A, W_1|W_2, Y_1^n) \\ &= H(W_2, A, W_1, Y_1^n, V^n) - H(V^n|W_2, A, W_1, Y_1^n) \\ &\quad - H(Y_1^n) - H(A, W_1|W_2, Y_1^n) \\ &= H(W_2, A, W_1|Y_1^n, V^n) + H(Y_1^n, V^n) - H(Y_1^n) \\ &\quad - H(V^n|W_2, A, W_1, Y_1^n) - H(A, W_1|W_2, Y_1^n) \\ &\stackrel{(q)}{\geq} H(V^n|Y_1^n) - H(V^n|W_2, A, W_1, Y_1^n) \\ &\quad - H(A, W_1|W_2, Y_1^n) \\ &\stackrel{(r)}{\geq} H(V^n|Y_1^n, U^n, X_1^n, T^n) - H(V^n|W_2, A, W_1, Y_1^n) \\ &\quad - \log |\mathcal{A}| - H(V^n|Y_2^n, S_2^n, U^n, X_1^n, T^n) \\ &\stackrel{(s)}{\geq} n \left[I(V; Y_2, S_2|U, X_1, T) - I(V; Y_1|U, X_1, T) \right] \\ &\quad - H(V^n|W_2, A, W_1, Y_1^n) \\ &\quad - \left[\max\{I(V; S_1|U, X_1, T), I(V; Y_1|U, X_1, T)\} \right. \\ &\quad \left. - I(V; Y_1|U, X_1, T) \right] \\ &\geq n \left[I(V; Y_2, S_2|U, X_1, T) \right. \\ &\quad \left. - \max\{I(V; S_1|U, X_1, T), I(V; Y_1|U, X_1, T)\} \right] \quad (96) \end{aligned}$$

where (q) follows from the non-negativity of entropy function; (r) follows from the fact that conditioning does not increase the entropy, the non-negativity of entropy function, and the fact that $H(A, W_1|W_2, Y_1^n) = H(A|W_2, Y_1^n) + H(W_1|A, W_2, Y_1^n) \leq H(A) \leq \log |\mathcal{A}|$, thanks to $H(W_1|A, W_2, Y_1^n) = 0$; (s) is because of Fano's inequality which implies that the term $H(V^n|W_2, A, W_1, Y_1^n)$ tends to zero for $n \rightarrow \infty$ (see [20]). The proof is completed. \square

ACKNOWLEDGEMENT

This work was partially supported by Iran National Science Foundation (INSF), under contracts' numbers 91/s/26278 and 92/32575. Parts of this paper was presented in the International Symposium on Information Theory and Application (ISITA) 2010.

The authors gratefully acknowledged the anonymous reviewers for their suggestions, comments and corrections as well as those of the associate editor.

REFERENCES

1. A. B. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 1, Jan. 1978.
2. Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–618, Feb. 2009.
3. R. Duan and Y. Liang, "Bounds and capacity theorems for cognitive interference channels with state," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 280–304, 2015.
4. P. Devroye, N. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1813–1827, May, 2006.
5. W. Wu, S. Vishwanath, and A. Arapostathis, "Capacity of a class of cognitive radio channels: interference channels with degraded message sets," *IEEE Trans. on Inf. Theory*, vol. 53, no. 11, pp. 4391–4399, Nov. 2007.
6. I. Maric, A. Goldsmith, G. Kramer, and S. Shamai, "On the capacity of interference channels with one cooperating transmitter," *European Trans. on Telecomm.*, vol. 19, no. 4, pp. 405–420, 2008.
7. S. Rini, D. Tuninetti, and N. Devroye, "New inner and outer bounds for the memoryless cognitive interference channel and some new capacity results," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4087–4109, July 2011.
8. S. Rini, D. Tuninetti, and N. Devroye, "Inner and outer bounds for the Gaussian cognitive interference channel and new capacity results," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 820–848, Feb. 2012.
9. S. Rini, E. Kurniawan and A. Goldsmith, "Combining superposition coding and binning achieves capacity for the Gaussian cognitive interference channel," *IEEE Inf. Theory Workshop (ITW)*, Jul. 2012, pp. 227–231.
10. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
11. A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
12. Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*, Now Pub. Inc., 2009.
13. H. G. Bafghi, S. Salimi, B. Seyfe, and M. R. Aref, "Cognitive interference channel with two confidential messages," in *Int. Symp. on Inf. Theory and Applic. (ISITA)*, Taichung, Taiwan, 2010, pp. 952–956.
14. R. K. Farsani and R. Ebrahimpour, "Capacity theorems for the cognitive radio channel with confidential messages," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, June 2014, pp. 1416–1420.
15. C. E. Shannon, "Channels with side information at the transmitter," *J. Res. Devel.*, vol. 2, pp. 289–293, 1958.
16. A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge University Press, 2011.
17. S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Probl. Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.
18. M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 439–441, May 1983.
19. A. Somekh-Baruch, S. Shamai, and Verdú S., "Cognitive interference channels with state information," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Toronto, Canada, July 6–11, 2008, pp. 1353–1357.
20. H. G. Bafghi and B. Seyfe, "On the secrecy of the cognitive interference channel with channel state," *Jour. of Comm. Eng. (JCE)*, vol. 2, no. 1, pp. 54–62, Winter 2013.
21. H. A. Suraweera, P. J. Smith, and M. Shafi, "Capacity limits and performance analysis of cognitive radio with imperfect channel knowledge," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 1811–1822, May 2010.
22. P. J. Smith, P. A. Dmochowski, H. A. Suraweera, and M. Shafi, "The effects of limited channel knowledge on cognitive radio system capacity," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 927–933, Feb. 2013.
23. W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proc. 41st Asilomar Conf. Signals, Systems and Comp.*, Pacific Grove, CA., Nov. 2007, pp. 893–897.
24. I. Maric, A. Goldsmith, G. Kramer, and S. Shamai, "On the capacity of interference channels with a partially-cognitive transmitter," *IEEE Int. Symp. on Inf. Theory (ISIT)*, pp. 2156–2160, June 2007.
25. I. Maric, A. Goldsmith, G. Kramer, and S. Shamai, "On the capacity of interference channels with a cognitive transmitter," *Inf. Theory and Applic. Workshop*, pp. 268–273, Jan. 2007.
26. A. Khisti, S. Diggavi, and G. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. Forens. and Sec.*, vol. 6, no. 3, pp. 672–681, Sept. 2011.
27. A. Jovičić and P. Viswanath, "Cognitive radio: An information theoretic perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3945–3958, 2009.
28. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
29. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 2nd edition, 2006.
30. R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.